UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/814,601	03/23/2001	James T. Lynn	GE04347	3710

43471 7590 02/23/2010

Motorola, Inc.
Law Department
1303 East Algonquin Road
3rd Floor
Schaumburg, IL 60196

EXAMINER	
DAVIS, ZACHARY A	

ART UNIT	PAPER NUMBER
2437	

NOTIFICATION DATE	DELIVERY MODE
02/23/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

Docketing.US@motorola.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte JAMES T. LYNN, TODD C. SHANEYFELT,
MICHAEL T. SMITH, and JAMES E. GREENWOOD, JR.

Appeal 2009-006712
Application 09/814,601
Technology Center 2400

Decided: February 19, 2010

Before MAHSHID D. SAADAT, CARLA M. KRIVAK, and
BRADLEY W. BAUMEISTER, *Administrative Patent Judges*.

KRIVAK, *Administrative Patent Judge*.

DECISION ON APPEAL

Appellants appeal under 35 U.S.C. § 134(a) from a rejection of claims 1-5. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

STATEMENT OF THE CASE

Appellants' claimed invention is a method for securely distributing software components on a computer network (Spec. 2:6-7). The method includes executing a secure kernel and a digitally signed configuration file containing a load table on a network appliance. The secure kernel verifies the authenticity of the configuration file and load table. (Abstract)

Independent claim 1, reproduced below, is representative of the subject matter on appeal.

> 1. A method for securely distributing a component from a network host to a network appliance, comprising the steps of:
>
> signing, by said network host, a configuration file including a load table which defines a plurality of authorized components for said network appliance;
>
> executing a secure kernel and said signed configuration file on said network appliance, said secure kernel including computer code for checking the authenticity of said configuration file and boot code for allowing said network appliance to initially boot up and establish communication with said network host;
>
> verifying, by said secure kernel, the authenticity of said configuration file;
>
> reading, by said secure kernel, said load table only after said verifying step; and
>
> loading said plurality of authorized components defined in said load table onto said network appliance.

REFERENCE

Slivka	US 6,049,671	Apr. 11, 2000 (filed Apr. 18, 1996)

The Examiner rejected claims 1-5 under 35 U.S.C. § 102(e) based upon the teachings of Slivka.

Appellants contend Slivka does not teach digitally signing, by a network host, a configuration file including a load table that defines a plurality of authorized components for the network appliance (Br. 4-6). Appellants further contend Slivka does not teach a host generating and signing an updated configuration file (Br. 6).

ISSUES

Did the Examiner err in finding Slivka teaches a configuration file including a load table that defines a plurality of authorized components for a network appliance?

Did the Examiner err in finding Slivka teaches a host generating and signing an updated configuration file?

FINDINGS OF FACT

1. Slivka teaches a computer software update service wherein a user has the option of choosing none, one, or a number of computer software components to download and install (Abstract; col. 8, ll. 57-59). When a user makes a request for software, e.g., a new or enhanced version of a network browser or other software, the server application 116 on the server computer 118 creates a file of directive commands 130 (col. 13, ll. 37-41). The file of directive commands is used to create a cabinet file and designate an installation program for installing the requested software (col. 13, ll. 44-46). Software is not downloaded without the user's permission (col. 8, ll. 46-47).

2. Slivka's cabinet file is "a grouping of files that are commonly conceptualized as being stored in an 'electronic filing cabinet'" (col. 13, ll. 46-49).

3. Slivka teaches an update service that automatically inventories a user computer to determine needed software or maintenance updates. Slivka discloses that by "making periodic calls to an update or network service, the user always has the most up-to-date computer software immediately available." (Abstract)

4. After Slivka's cabinet file is combined with a self extracting application program (WEXTRACT), a resulting self-extracting, executable distribution file is digitally signed with a digital signature to create a signed, self-extracting executable distribution file 136 (col. 16, ll. 55-58).

PRINCIPLES OF LAW

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros., Inc. v. Union Oil Co. of Calif.*, 814 F.2d 628, 631 (Fed. Cir. 1987).

ANALYSIS

The Examiner rejected claims 1-5 under 35 U.S.C. § 102(e) as anticipated by Slivka (Ans. 3). Appellants argue this rejection with respect to claims 1 and 5.

Claim 1

Appellants contend Slivka does not teach a configuration file including a load table that defines a plurality of authorized components for a

network appliance because Slivka appears to be nothing more than an on-line store (Br. 4-6). That is, Slivka allows "a user to pick and choose any program desired regardless of whether or not the network appliance is authorized to use the program" (Br. 5).

The Examiner finds Slivka's cabinet file corresponds to Appellants' configuration file. Slivka's cabinet file includes an installation table that lists files included within the cabinet file. Appellants' load table lists software components within a configuration file (Ans. 5, FF 2). Thus, Appellants' configuration file reads on Slivka's file cabinet.

The Examiner also finds Slivka's cabinet file includes software authorized by the user and requested for download (Ans. 5; FF 1, 2). That is, as Slivka teaches, a user chooses (authorizes) software, shown in an output report, to be downloaded (FF 1; col. 8, ll. 43-47). Thus, as Appellants note, Slivka is not concerned with whether a network appliance is authorized to use a program (Br. 5). However, claim 1 merely requires the components to be authorized, not the network appliance (Ans. 6). Thus, Slivka teaches the software components in the file cabinet are authorized.

For the above reasons, Slivka anticipates claim 1.

Claim 5

The Examiner rejected claim 5 under 35 U.S.C. § 102(e) as anticipated by Slivka (Ans. 3). Appellants contend Slivka does not teach generating and signing an updated configuration file (App. Br. 6).

Slivka teaches a user can make periodic calls to an update service to obtain the most up-to-date computer software available (FF 3). Updating a summary of available software in the cabinet file, as taught by Slivka, would effectively alter the components a user can authorize for download and

would "constitute an updating of the configuration file" as claimed (Ans. 9). The server then digitally signs Slivka's updated cabinet file (Ans. 9-10; col. 17, ll. 57-60; FF 4). Thus, Slivka teaches generating and signing an updated configuration file.

CONCLUSION

The Examiner did not err in finding Slivka teaches a configuration file including a load table that defines a plurality of authorized components for a network appliance.

The Examiner did not err in finding Slivka teaches a host generating and signing an updated configuration file.

DECISION

The Examiner's decision rejecting claims 1-5 is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

KIS

Motorola, Inc.
Law Department
1303 East Algonquin Road
3rd Floor
Schaumburg, IL 60196